

REMARKS

The Office Action in the above-identified application has been carefully considered and this amendment has been presented to place this application in condition for allowance.

Accordingly, reexamination and reconsideration of this application are respectfully requested.

Claims 1-4 and 6-9 are in the present application. It is submitted that these claims, are patentably distinct over the prior art cited by the Examiner, and that these claims are in full compliance with the requirements of 35 U.S.C. § 112. Changes to the claims, as presented herein, are not made for the purpose of patentability within the meaning of 35 U.S.C. sections 101, 102, 103 or 112. Rather, these changes are made simply for clarification and to round out the scope of protection to which Applicants are entitled. Claim 5 is canceled.

The Specification was objected to because the title of the invention was not descriptive. In response, a new title is submitted that is clearly indicative of the invention to which the claims are directed. Accordingly, Applicants believe this objection has been overcome.

Claims 1-9 were rejected under 35 U.S.C. § 102(b) as being anticipated by Michener et al. (U.S. Patent 5,671,283). A distinguishing feature of the invention is "said CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value generating key." (Claims 1 and 6-9) This feature is disclosed in the specification by:

A flowchart of a data-integrity-check process using an ICV is shown in FIG. 15. In step S11, data to be treated by integrity checking is extracted. In step S12, based on the extracted data, a content check value 'ICV' is calculated by the DES cryptosystem construction shown in FIG. 14. In step S13, the calculated content check vale 'ICV' is

compared with an ICV stored in the data. If both values are equal to each other, the process determines that the data is free of interpolation and is correct (steps S14 to S15). If both values are not equal, the process determines that the data have been interpolated (steps S14 to S16).

.(See page 49, lines 14-24) and

In FIG.32, the construction of key encryption processing in the CBC mode is shown. This encryption processing is executed by the cryptosystem unit 236 (shown in FIG. 2) in media 2. The exclusive OR operation of the initial value 'IV_keys' stored in the internal memory 235 and the encrypted result is stored as 'Kicv_cont' is executed. The result is processed by performing DEC encryption to which the storage key 'Ksto' stored in the internal memory 235 is applied, and the encrypted result is stored as "Kicv_cont Encrypted' in the header. The exclusive OR operation of 'Kicv_cont Encrypted" and the content key Kc(0) corresponding to sector (0) is executed. The result is processed by performing DES encryption to which the storage key 'Ksto' stored in the internal memory 235 is applied, and the encrypted result is used as an encryption key 'Kc(0)Encrypted' to be stored in the header. The exclusive OR operation of the 'Kc(0)Encrypted' and the content key 'Kc(1)' is executed. The result is processed by performing DES encryption to which the storage key 'Ksto' stored in the internal memory 235 is applied, and the encrypted result is represented by 'Kc(1)Encrypted'. After that, by repeatedly executing these steps, key data to be stored in the header is formed.

(See page 86, line 9 to page 87, line 6). Applicants believe this distinguishing feature of the present invention is not disclosed in Michener. Accordingly, Michener fails to anticipate the present invention and the rejected claims should now be allowed.

In view of the foregoing amendment and remarks, it is respectfully submitted that the application as now presented is in condition for allowance. Early and favorable reconsideration of the application are respectfully requested.

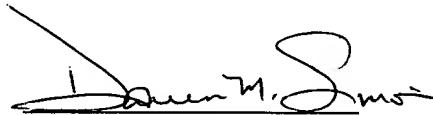
An extension of time fee is deemed to be required for the filing of this amendment. No additional fees are anticipated, but if such are required, the Examiner is hereby authorized to

charge any insufficient fees or credit any overpayment associated with the above-identified application to Deposit Account No. 50-0320.

If any issues remain, or if the Examiner has any further suggestions, he/she is invited to call the undersigned at the telephone number provided below. The Examiner's consideration of this matter is gratefully acknowledged.

Respectfully submitted,
FROMMER LAWRENCE & HAUG LLP

By:

A handwritten signature in black ink, appearing to read "Darren M. Simon", written over a horizontal line.

Darren M. Simon
Reg. No. 47,946
(212) 588-0800